
DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

# Monthly Report to Congress of Data Incidents

## April 29 - June 2, 2013

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000088611 | Mishandled/ Misused Physical or Verbal Information | VBA St Petersburg, FL | 4/29/2013 | 4/30/2013 | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0589258 | 4/29/2013 | INC000000278832 | N/A | N/A | N/A | 2 | |

**Incident Summary**

A letter sent to Veteran A included one document for Veteran B and one document for Veteran C.

**Incident Update**

04/24/13:
Due to full SSN being exposed, Veterans B and C will be sent a letter offering credit protection services.

**NOTE: There were a total of 133 Mis-Mailed incidents this reporting period. Because of repetition, the other 132 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.**

**Resolution**

We spoke to all Mailroom and Service Center employees on the importance of double-checking all mail being sent out especially Veterans Claims Assistance Act of 2000 (VCAA) letters. We will continue to monitor this issue on a daily basis with our employees.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000088615 | Mishandled/ Misused Physical or Verbal Information | VISN 09 Nashville, TN | 4/29/2013 | 5/13/2013 | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0589262 | 4/29/2013 | INC000000278921 | N/A | N/A | N/A | | 270 |

**Incident Summary**

On Thursday, 04/25/13, at 9:00 AM, the Program Assistant, Compliance Office (Nashville Campus) found a Gains and Losses (G&L) sheet in the men's restroom (B-111). The G&L sheet contained the full name, last four digits of the SSN, and ward location for approximately 90 Veterans. The Program Assistant, Compliance Office (Nashville Campus) placed the G&L sheet in the shredder box.

Today, 04/29/13, at 9:00 AM, the Program Assistant, Compliance Office (Nashville Campus) found three (3) G&L sheets in the men's restroom (B-102). G&L sheets contained the full name, last four digits of the SSN, and ward location for approximately 180 Veterans.

The G&L sheets are utilized in morning report. It is believed the G&L sheets were inadvertently left in the restrooms by an employee who attended morning report on the dates in question. Morning report ends at approximately 8:45 AM so the G&L sheets were left unattended for a very short period.

**Incident Update**

04/29/13:
Due to the fact that ward location is considered Protected Health Information (PHI), 270 Veterans will receive notification letters.

**Resolution**

It is believed the G&L sheets were inadvertently left in the staff restrooms by an employee(s) who attended the morning meeting. HIPAA notification letters were mailed today. Staff has been reminded of the importance of safeguarding patient information to include the appropriate process for disposal of such documents.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000088693 | Mishandled/ Misused Physical or Verbal Information | VHA CMOP Hines, IL | 4/30/2013 | 5/9/2013 | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0589339 | 4/30/2013 | INC000000279386 | N/A | N/A | N/A | | 1 |

**Incident Summary**

Patient A received a prescription intended for Patient B. Patient B's name, address, and type of medication were compromised. Patient A reported the incident to the medical center and a replacement has been requested for Patient B. Great Lakes Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee will be counseled and retrained in proper packing procedures.

**Incident Update**

05/01/13:
Patient B will be sent a HIPAA notification letter due to Protected Health Information (PHI) being disclosed.

**NOTE: There were a total of 4 Mis-Mailed CMOP incidents out of 7,796,989 total packages (11,547,075 total prescriptions) mailed out for this reporting period. Because of repetition, the other 3 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.**

**Resolution**

The CMOP employee was counseled and retrained in proper packing procedures.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000088839 | Mishandled/ Misused Physical or Verbal Information | VISN 08 Tampa, FL | 5/3/2013 | 6/3/2013 | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0589478 | 5/3/2013 | INC000000280221 | N/A | N/A | N/A | 29 | |

**Incident Summary**

A clerk left an unsecured stack of consults on top of a desk while at lunch. The consults were missing upon the clerk's return. A search of the area and employees did not turn up the documents.

**Incident Update**

05/03/13:
Twenty nine Veterans will be sent letters offering credit protection services, as their full SSN, date of birth, and other medical information were disclosed.

**NOTE: There were a total of 141 Mis-Handling incidents this reporting period. Because of repetition, the other 140 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.**

**Resolution**

The investigation, remediation, and sanctions were completed. The employee received written counseling.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000088847 | Missing/Stolen Equipment | VISN 11 Detroit, MI | 5/3/2013 | | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0589485 | 5/3/2013 | INC000000280233 | N/A | N/A | N/A | | |

**Incident Summary**

During an OIT inventory, there were three PC workstations on the equipment inventory list (EIL) that were not found. .

**Incident Update**

05/03/13:
The Chief Information Officer (CIO) is investigating the three PCs, which were believed to be used as patient internet access computers because they have not checked into the network. The PCs were not encrypted. A Report of Survey was submitted.

**NOTE: There were a total of 2 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 1 is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.**

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000089121 | Missing/Stolen Equipment | VISN 07 Decatur, GA | 5/10/2013 | | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0589760 | 5/10/2013 | INC000000282039 | N/A | N/A | N/A | | |

**Incident Summary**

A VA employee reports that a VA computer is missing or stolen.

**Incident Update**

06/05/13:
After further investigation, the desktop PC was determined to have been stolen. The PC was password protected and encrypted. It was used in and stolen from the Primary Care section of the hospital. It was used for patient check-in. There was no sensitive information stored on the PC. The VA Police were contacted regarding this on 05/10/13 and a Police report was made. The PC has not been recovered.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000089127 | Mishandled/ Misused Physical or Verbal Information | VISN 08<br>West Palm Beach, FL | 5/10/2013 | | Medium |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0589765 | 5/10/2013 | INC000000282084 | N/A | N/A | N/A | | 63 |

**Incident Summary**

A VA driver left a roster of Special Mode Transportation patients in a public location.

**Incident Update**

05/10/13:
The list was left on a counter at a McDonald's restaurant. There were 63 Veterans affected. The information on the list included name, last four digits of the SSN, and diagnoses. The 63 Veterans will be sent HIPAA notification letters.

**Resolution**

The VA driver has returned to the location and retrieved the paperwork. He will return it to the Transportation Supervisor tomorrow (Saturday) morning. The Supervisor will give it to the Privacy Officer (PO) on Monday morning. The Transportation Supervisor will review procedures and proper handling of sensitive information with the employee.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000089551 | Missing/Stolen Equipment | VISN 03 New York, NY | 5/21/2013 | | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0590184 | 5/21/2013 | INC000000284684 | N/A | N/A | N/A | | |

**Incident Summary**

Research confirmed that two hard drives are missing for a protocol. The hard drives were located in room 16027 at the New York Harbor Health Care System (NYHHCS) Manhattan Campus. A main door to the wing was unlocked as well as the door to the room where the external hard drives where stored. The Research doctor stated that the data was coded and no VA sensitive information was at risk. A VA Police Report was generated.

**Incident Update**

05/22/13:
The hard drives were not encrypted. The Privacy Officer (PO) has confirmed that the data on the drive was de-identified. Police are looking through video surveillance tapes to see if any new information can be obtained on the equipment.

05/23/13:
The Information Security Officers (ISO) reviewed the protocol linked to this incident. The ISOs are looking at the issues in the Human Studies Questionnaire (HSQ) including using unencrypted external drives. The ISOs have requested an interview with the Primary Investigator (PI) to look at the data on the Research computer (the external drives were used to back up the data on this computer.) The ISOs are trying to verify the data is not VA sensitive.

06/03/13:
An ISO at the NYHHCS Manhattan Campus has confirmed that the data on the computer was indeed de-identified (it contained only numbers that had been generated by another piece of equipment, with nothing to connect the number to any individual).

Confirmation from has come from the PI that the drives are not VA owned. The protocol is coming up for continuing review on 06/03/13. The PI/Research must request that NYU allow the NYHHCS CIO to administrative rights on the machine and external hard drives for encryption. If this cannot be done an Institutional Review Board (IRB) will have to determine another way to maintain this protocol in a secure manner or deny the continuation until compliant with VA 6500 and Research policies and regulations. The ISO is meeting with Research and arranging a conference with the PI at this time. The Additional education will be administered by the ISO and PO to the PIs and the Research department to aid them in compliance with all VA 6500, Privacy, HIPAA, and Research policies.

| Security Privacy Ticket Number | Incident Type | Organization | Date Opened | Date Closed | Risk Category |
|---|---|---|---|---|---|
| PSETS0000089571 | Missing/Stolen Equipment | VISN 18 Tucson, AZ | 5/21/2013 | | Low |

| VA-NSOC Incident Number | Date US-CERT Notified | US-CERT Case Number | Date OIG Notified | Reported to OIG | OIG Case Number | No. of Credit Monitoring | No. of Loss Notifications |
|---|---|---|---|---|---|---|---|
| VANSOC0590204 | 5/21/2013 | INC000000284739 | N/A | No | N/A | | |

**Incident Summary**

A computer is missing from the last location where it was inventoried. It was never connected to the VA network, and was used to print physical therapy instructions for patients. It was last inventoried in December 2011. There may be patient names and diagnoses on the hard drive. It was a Windows XP computer and not encrypted.

**Incident Update**

05/22/13:
A complete survey of the areas where the computer was used, including all the storage areas was completed. The computer was used by the physical therapy section to create copies of therapeutic exercises for patients. Although it had the ability to enter patient names, few users did. The computer was underutilized, especially after the software program was moved to the network to expand its accessibility. No records of the turn in sheets for the equipment or the computer were found. A complete search of the facility has been performed and the PC search has concluded. Per the Information Security Officer (ISO), the only personally identifiable information (PII) or protected health information (PHI) that would have been stored on the computer would be names.

06/04/13:
Additional update from the ISO indicates that the software on the computer does not store the name, nor is there a database lookup that would tie an entered name to anything. Also, the exercises that could be printed out would indicate a general focus for the exercise, i.e. back, arms, legs, but nothing specific to indicate whether it was weakness, pain, stroke, surgery, or other reason for the therapy.

**Resolution**

On 05/21/13, Computer and Biomed staff were reminded of the requirement to physically secure stand-alone PC's that contain patient information.

| | |
|---|---|
| Total number of Internal Un-encrypted E-mail Incidents | 111 |
| Total number of Mis-Handling Incidents | 141 |
| Total number of Mis-Mailed Incidents | 133 |
| Total number of Mis-Mailed CMOP Incidents | 4 |
| Total number of IT Equipment Inventory Incidents | 2 |
| Total number of Missing/Stolen PC Incidents | 5 |
| Total number of Missing/Stolen Laptop Incidents | 7 (7 encrypted) |
| Total number of Lost BlackBerry Incidents | 16 |
| Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents | 2 |